UNIVERSITÀ POLITECNICA DELLE MARCHE

FACOLTÀ DI ECONOMIA "GIORGIO FUÀ"

Corso di Laurea triennale in Economia Aziendale

L' ERA DELLE CRIPTOVALUTE:

IL MERCATO DEI BITCOIN

THE ERA OF CRYPTOCURRENCIES:

THE BITCOIN MARKET

Relatore:

Prof. Filippo Fiordiponti

Tesi di Laurea di:

Cardinali Riccardo

Anno Accademico 2019/2020

INDICE

Capitolo 1- ASPETTI GENERALI DEL BITCOIN 4

1.1 La crittografia 5

1.2 La funzione Hash 7

1.3 Le firme digitali 8

1.4 Blockchain 9

1.5 Transazioni 11

1.6 Moneta 13

Capitolo 2- IL MINING **14**

2.1 Il double spending 15

2.2 Fee delle transazioni 17

2.3 L'algoritmo di mining 18

Capitolo 3- GENERAZIONE DEI BITCOIN **20**

Capitolo 4- I MERCATI OTC **23**

4.1 Il mercato Forex 24

Capitolo 5- ANALISI DI PREZZO DI BITCOIN **26**

Capitolo 6- L'ANALISI TECNICA **29**

6.1 Il grafico a candela 30

6.2 I principi fondamentali dell'analisi tecnica 31

6.3 Supporti e resistenze 33

6.4 Le medie mobili 34

6.5 Le Bande di Bollinger 35

6.6 Il Percentage B o "%b" 37

6.7 Bandwidth 37

6.8 Il Williams %R 38

6.9 Il Parabolic SAR 39

Capitolo 7- TRADING SYSTEM E BITCOIN 40

7.1 Trading system con le medie mobili 41

7.2 Trading system con le Bande di Bollinger 42

7.3 Trading system con Williams %R 43

7.4 Trading system con il Parabolic SAR 44

INTRODUZIONE

I bitcoin, così come le criptovalute in generale, stanno assumendo un ruolo sempre più centralizzato e, in un mondo che si avvia verso una fase in cui le operazioni vengono compiute digitalmente e in maniera più rapida, i presupposti per diventare tra i più importanti mezzi di scambio non mancano. A ragione di quanto detto, questa tesi mira a presentare il mondo Bitcoin, dagli aspetti generali che lo compongono e i vari meccanismi che permettono il suo funzionamento fino ad arrivare alla loro applicazione nel mercato. Verranno affrontati varie tematiche, anche domande che possono sorgere quando ci si addentra in questo settore, come il comprendere se i bitcoin possono essere considerati una moneta, le modalità di transazione la remunerazione di chi opera con questa tipologia di valuta.
Sicuramente l'analisi che verrà proposta non sarà delle più esaustive, su questa tematica possono essere scritti volumi su volumi, ma verranno affrontati i punti principali che permetteranno al meglio di comprendere lo scenario del Bitcoin.

CAPITOLO 1

ASPETTI GENERALI DEL BITCOIN

Prima di poter elencare i concetti che ruotano intorno al Bitcoin, occorre dare una definizione a quella che, negli anni, è diventata una criptovaluta di un'importanza tale da suscitare anche l'interesse dei meno esperti in materia. Una definizione esauriente può essere presa da Wikipedia:

Bitcoin è un sistema di pagamento peer-to-peer e una moneta digitale, sviluppato nel 2009 come software open source. Si tratta di una crypto valuta, poiché utilizza la crittografia per controllare la creazione e il trasferimento della moneta. Convenzionalmente la parola "Bitcoin", scritta in maiuscola, si riferisce alla tecnologia e al network, mentre la parola "bitcoin" scritta in minuscolo, si riferisce alla valuta stessa.

Il termine Bitcoin comprende tre concetti fondamentali:

- Bitcoin è un protocollo.
- Bitcoin è un progetto software open source.
- Bitcoin è un network.

Il Bitcoin è un protocollo, ovvero un insieme di regole che servono a definire il funzionamento del software utilizzato da un network di computer collegati tra loro, con lo scopo di creare e gestire la valuta bitcoin. Comprendere il protocollo

Bitcoin è molto complesso e richiede specifiche conoscenze di programmazione e crittografia, ma occorre passare per determinati punti in modo tale da poter entrare nell' ottica di funzionamento di questo sistema. I punti d' interesse sono:

- Crittografia.
- Funzione Hash.
- Firme digitali.
- Blockchain.
- Transazioni.

1.1 La crittografia

La crittografia è importante che venga discussa come primo punto, perché, oltre al funzionamento, quest' ultima è legata al sistema di sicurezza del network Bitcoin. Essendo una moneta digitale, molti presentano i propri dubbi riguardo la facilità con cui utenti esterni possano accedere a determinati dati, ma si vedrà ben presto che il sistema ha una struttura difficilmente attaccabile. La crittografia è un insieme di tecniche che consentono di trasmettere un messaggio mantenendolo segreto a tutti, tranne alle persone che possiedono le chiavi per decifrarlo. In poche parole, il suo scopo è quello di mantenere nascosto il contenuto del messaggio. Due sono gli elementi che caratterizzano un codice di cifratura, ovvero l'algoritmo e la chiave. L' algoritmo è la regola tramite la quale il messaggio originale viene modificato, rendendolo criptato, mentre la chiave è il parametro

che permette di decodificare il messaggio. In un metodo di cifratura simmetrico, la chiave per codificare e decodificare il messaggio è la stessa. Quando si parla di Bitcoin, il metodo di cifratura utilizzato è di tipo asimmetrico, il quale presenta maggiori vantaggi rispetto alla cifratura simmetrica. La differenza essenziale è data dall' introduzione di due chiavi: una pubblica e una privata.
La chiave pubblica è nota a tutti coloro che vogliono inviare un messaggio cifrato, mentre la chiave privata è nota solo al destinatario ed è l'unico strumento a disposizione per decifrare il messaggio ricevuto. In questo modo un mittente "A", per cifrare il messaggio, utilizza la chiave pubblica del destinatario, mentre il ricevente "B" potrà essere l'unico a decifrarlo con la propria chiave privata. Il problema potrebbe presentarsi nel caso in cui un soggetto C, durante la trasmissione del messaggio, possa intercettarlo e sostituirlo con un altro. In tale situazione, B non avrebbe modo di sapere se il suo messaggio sia l'originale.
Tutto questo in linea teorica, perché, come detto in precedenza, Bitcoin ha un sistema di sicurezza molto elevato e le transazioni che avvengono tra gli utenti hanno un'elevata difficoltà di poter essere ostacolate. Difatti l'utente A utilizza la chiave pubblica di B per cifrare il messaggio e lo autentica con la propria chiave privata. In questo modo avviene una doppia cifratura. L' autenticità della prima può essere verificata da tutti, ma riguardo la seconda solo B potrà effettuare la verifica tramite la propria chiave privata. Tramite questi passaggi è possibile garantire sicurezza, integrità, autenticità e accettazione. Non finisce qui, infatti è

possibile aumentare il grado d' integrità e autenticità del messaggio tramite la funzione Hash.

1.2 La funzione Hash

La funzione Hash è un sistema che trasforma un messaggio di lunghezza arbitraria in un codice alfanumerico di lunghezza prefissata, che prende il nome di Hash. Questa funzione presenta le seguenti caratteristiche:

- Semplicità: il calcolo del codice Hash deve essere sempre agevole.
- Univocità: la probabilità che due messaggi generino lo stesso codice Hash è nulla.
- Non convertibilità: è impossibile risalire al codice Hash del messaggio.
- "Effetto valanga": una minima modifica del messaggio comporta una profonda alterazione dell'Hash.

La funzione dell'Hash è, quindi, di identificare in modo univoco e irreversibile un messaggio, conferendogli integrità e autenticità. Se si vuole creare un proprio messaggio (esempio: "compra 50 bitcoin") e applicando l'algoritmo preso dal sito www.hashemall.com, si otterrà un codice Hash di 64 caratteri. La semplice sostituzione di una lettera del messaggio "compra 50 bitcoin" comporterà una modifica radicale del codice, in accordo con il principio "effetto valanga".

1.3 Firme digitali

La crittografia e le funzioni Hash trovano applicazione nel campo delle firme digitali. Il soggetto A applica una funzione Hash sul messaggio, ottenendo il codice di 64 caratteri che cifra usando la chiave privata. Si ottiene in questo modo la firma. Di conseguenza documento e firma vengono inviati al destinatario. Nel momento in cui B riceve, separa il messaggio in documento originale e firma digitale e, tramite la chiave pubblica del mittente, è in grado di decifrare la firma digitale ottenendo l'Hash. Successivamente, applicando al documento originale la medesima funzione Hash potrà valutare l'autenticità del messaggio nel caso in cui l'Hash ottenuto è uguale a quello appena decifrato.

Finora abbiamo parlato, seppur in maniera semplificata, di come il sistema Bitcoin garantisca un elevato livello di sicurezza tra gli utenti, dal momento in cui il messaggio viene creato e viene assegnato il codice univoco, fino al momento della ricezione, decodificazione e autenticazione. Questo però non è altro che una piccolissima parte delle enormi funzionalità che si trovano dietro Bitcoin. Nel prossimo paragrafo, infatti, verrà introdotto il Blockchain, che possiamo quasi considerare la base che sopporta l'intero sistema.

1.4 Blockchain

Il Blockchain è il registro pubblico di tutte le transazioni e queste sono contenute in blocchi ordinati cronologicamente. Blockchain, infatti, vuol dire "catena di blocchi", non a caso ogni blocco è collegato al precedente. Di conseguenza è facile capire che, svolgendo un percorso a ritroso, si può risalire la catena fino ad arrivare al numero 0, ovvero il "Genesis Block", nato alle ore 18:15:05 del 3 gennaio 2009. Il Blockchain quindi funge da database che comprende tutti i blocchi genrati e le varie transazioni effettuate. Arrivati a questo punto occorre spiegare cosa sia un blocco. Il blocco, molto semplicemente, è un file in cui sono contenute una serie di informazioni, di cui le più importanti sono:

- Numero del blocco: i blocchi sono numerati in ordine crescente.
- Codice Hash: come abbiamo già discusso nei precedenti paragrafi, ogni blocco è identificato in maniera univoca da un codice alfanumerico.
- Data e ora in cui il blocco è stato prodotto.
- Tutte le transazioni confermate nel blocco.
- Totale bitcoin movimentati all' interno del blocco.
- Dimensione (in KB) del blocco.

Un blocco, quindi, contiene un certo numero di transazioni. Di conseguenza un aumento della dimensione media dei blocchi riflette un aumento delle transazioni contenute al loro interno. Inoltre, la transazione ha un input e un

output, i quali rispettivamente ci segnalano da dove arrivano i bitcoin e verso dove sono diretti. La quantità assegnata ad ogni blocco è 50 bitcoin, ma si dimezza ogni 210.000 blocchi. Nel blocco attuale vengono assegnati 25 bitcoin. Da qui verrà preso in esame lo script, ovvero il linguaggio che accompagna le transazioni in modo da costituire i nodi per realizzare operazioni più complesse del semplice trasferimento. Lo script è composto dalla firma digitale e dalla chiave pubblica. La chiave pubblica appartiene al beneficiario dell'output della transazione, in modo tale che egli possa riscattare il valore di moneta. La firma digitale riguarda precisamente la firma dell'Hash che, combinata con la chiave pubblica, dimostra che la transazione sia stata eseguita del legittimo proprietario dell'indirizzo in oggetto. Analizzando i vari aspetti che compongono Bitcoin, è impossibile non fare caso a come chiave pubblica e chiave privata siano essenziali e permettano di passare da una fase all'altra riducendo il pericolo di attacchi esterni. Come le transazioni, anche le chiavi hanno un luogo elettronico in cui vengono conservate, ovvero il wallet. Il wallet viene definito come un portafoglio elettronico che memorizza tutte le credenziali digitali per accedere, spendere e trasferire i bitcoin. Si elencano 3 tipologie di wallet:

- il desktop wallet: un client che si installa sul proprio computer;
- lo smartphone wallet: è un'app che permette di effettuare e ricevere; pagamenti

- il web wallet: è un'account che permette di accedere al wallet del proprio browser.

Verrà presentato il più sicuro di tutti i wallet. Con "Cold Storage" si definisce una serie di bitcoin presenti su un wallet creato e mantenuto offline. Questo rappresenta il metodo di protezione più efficiente: nel caso in cui un PC subisca un attacco hacker, tale intrusione non risulterebbe pericolosa in quanto le chiavi private di accesso al wallet dell'utente non sarebbero più presenti sul dispositivo, ma sarebbero al sicuro offline.

1.5 Transazioni

Rispetto ai tradizionali sistemi di pagamento, all' interno dei quali ogni volta che viene effettuato un acquisto c' è bisogno di un intermediario che funga da garante dietro compenso, Bitcoin è caratterizzato da un sistema di pagamento elettronico basato su prove di crittografia, piuttosto di fiducia. L'utilizzo dei bitcoin permette una grandissima riduzione dei costi di transazione, aspetto da non sottovalutare dato che la tariffa standard si aggira intorno al 3,4 % dell'importo. Una soluzione comune al fine di tutelare il destinatario in una transazione è l'introduzione di un'autorità centrale che controlli ogni transazione ed eviti il double-spending, come la Zecca. Il problema di questa soluzione è che l'intero sistema monetario dipenda dalla società che gestisce la Zecca, che nei sistemi economici è lo Stato. Bitcoin ha voluto evolvere questa tipologia di sistema, evitando la presenza di una

terza parte di fiducia e al tempo stesso garantire la doppia spesa. Per poter realizzare ciò, è necessario un network di partecipanti in cui le transazioni vengano annunciate pubblicamente e questi ultimi si occupino di confermare l'ordine delle varie transazioni. Ipotizziamo che A sia intenzionato ad acquistare un certo bene e che il venditore B accetti bitcoin come sistema di pagamento. Ciò che l'acquirente dovrà fare è inviare una transazione verso l'indirizzo che identifica il portafoglio del beneficiario. Nel wallet è presente la chiave privata per firmare le transazioni. Il soggetto A, che intende trasferire i propri bitcoin, non fa altro che firmare l'Hash della precedente transazione e aggiungere la chiave pubblica del nuovo proprietario. Successivamente, la transazione passa nel network Bitcoin e il resto dei nodi valida le firme crittografiche. La transazione in questo modo è:

- Irreversibile: non è più annullabile.
- Pubblica: è tracciabile nel Blockchain.
- Anonima per le parti che l'hanno eseguita.

Da qualsiasi parte è possibile ricevere o effettuare pagamenti, con la semplice immissione dell'importo e l'autorizzazione da parte del cliente, in pochi minuti si potrà constatare l'importo richiesto sul proprio wallet.

1.6 Moneta

La moneta è l'insieme dei valori che vengono utilizzati per acquistare beni e servizi. La moneta svolge tre funzioni:

- Mezzo di scambio
- Unità di conto
- Riserva di valore

Oltre questo, sono riconosciuti due tipi di moneta: moneta merce e moneta a corso legale. La prima è una forma materiale di moneta rappresentata da un bene dotato di un proprio valore intrinseco (l'esempio classico è rappresentato dall' oro). La seconda, invece, non ha valore intrinseco e il suo valore è dettato dallo Stato. Dopo questa breve presentazione dei concetti fondamentali che riguardano la moneta, occorre comprendere la relazione con i bitcoin. Basandoci sugli aspetti appena citati, non possiamo considerare il bitcoin né una moneta merce, poiché privo di un proprio valore intrinseco, né una moneta a corso legale, poiché non esiste autorità centrale che la controlli. Quindi, nonostante il bitcoin svolga le tre funzioni principali della moneta, non è possibile considerarla tale. Una dimostrazione del fatto che moneta e bitcoin operino in maniera differente può essere data dal caso in cui, all' interno di un sistema monetario, la situazione diventi insostenibile e, per la ricollocazione ottimale delle risorse, le banche decidano di attuare una politica che vada a diminuire l'offerta di moneta e ad innalzare i tassi d'interesse. Dal

lato dei bitcoin l'offerta è limitata a 21 milioni e questo rende impossibile perseguire tali politiche.

CAPITOLO 2

IL MINING

Nello scorso capitolo è stato analizzato il Bitcoin sotto un punto di vista tecnico, prendendo uno ad uno gli elementi che lo caratterizzano e comprendendo cosa permette al sistema di operare. Da questo capitolo in avanti si analizzerà questo argomento da un punto di vista maggiormente funzionale, prendendo in considerazione cosa ha da offrire il mondo Bitcoin. Partendo da questo presupposto, è obbligatorio introdurre il "mining", un aspetto vitale dell'intera struttura Bitcoin. Il processo di mining, oltre a verificare e registrare tutte le transazioni, svolge l'attività di creare nuovi bitcoin. Oltre questo, è necessario elencare le tre attività svolte dal mining che permettono il funzionamento del network:

- Permette la verifica delle transazioni e la convalida dei blocchi.
- Previene il double spending.
- Raccoglie le fee delle transazioni.

Riguardo il primo punto, la verifica delle transazioni e la convalida dei blocchi sono stati affrontati nel primo capitolo, quindi si passerà direttamente alla prevenzione del double spending.

2.1 Il double spending

Il double spending si verifica quando i bitcoin vengono spesi più di una volta. Nel paragrafo 1.5 è stato già accennato questo problema e di come un'autorità centrale sarebbe in grado di risolvere il problema, ma è stato anche detto che nel mondo Bitcoin quest' ultima sia assente. Di conseguenza, il double spending rappresenta uno dei problemi più gravi delle valute virtuali, infatti esse possono essere clonate e spese più volte. Il mining, come già detto, è un sistema distribuito di consensi sulle transazioni avvenute, mentre il Blockchain è il libro contabile. Ogni volta che avviene una transazione, viene comunicato agli altri utenti del network la volontà di spostare n bitcoin da un determinato wallet. Gli utenti, seccessivamente, provvederanno a:

- verificare la validità della richiesta;
- verificare che il wallet contenga davvero n bitcoin;
- includere la transazione nel prossimo blocco che mineranno.

Tutta questa operazione non è istantanea ai vari utenti in Rete. Dopo "x" secondi dalla dichiarazione di transazione, ci saranno dei nodi del network che ne saranno a conoscenza, mentre altri no: i primi includeranno la transazione nel prossimo blocco da minare (termine utilizzato in italiano analogo a "mining", riguarda infatti la convalida delle transazioni), i secondi no. La domanda che sorge è: quando entrambi troveranno la soluzione al loro blocco e lo propagheranno, quale verrà accettata come la prossima sequenza valida

nel Blockchain? Il network accetterà il blocco o la serie di blocchi che ha richiesto il maggior lavoro per essere minata. Nel caso in cui un'entità "K" controlli il 51% di Hash rate (verrà ritrattato anche in seguito) del network si verificherebbe il caso in cui K sarebbe in grado non solo di minare i blocchi restanti, ma anche di decidere arbitrariamente quali transazioni possano realmente avere luogo nel network. Per dare un esempio pratico, si ipotizzi che K possieda realmente x bitcoin ed effettui una transazione verso un'entità J per un determinato valore di bitcoin al fine di acquistare un bene. Da qui, il network includerà la transazione nel suo prossimo blocco e comincerà a minarlo. Da una parte, J vedrà che il network ha minato un blocco contenente la transazione di bitcoin verso un suo wallet e procederà all'invio del bene a K, mentre quest'ultimo minerà da solo un blocco contenente una transazione in cui invia lo stesso ammontare x di bitcoin a sé stesso. Nel momento in cui K propagherà il blocco o la serie di blocchi contenenti la transazione maligna, il network accetterà questi al posto dei primi, in quanto è stato richiesto maggior lavoro e maggiore tempo. Il risultato di questa ipotesi è la perdita del bene acquistato con x bitcoin da parte di J. Si considera questo caso come l'unico attacco in grado di ledere realmente il network. Tuttavia bisogna tenere in considerazione due aspetti:

- l'attaccante non può effettuare transazioni da wallet di cui non conosce la chiave privata, quindi non può accaparrarsi bitcoin in possesso da altri

- l’attaccante non può creare bitcoin oltre il limite di 21 milioni.

2.2 Fee delle transazioni

In questo paragrafo verrà affrontato il motivo che spinge gli utenti a minare il sistema. Il mining, infatti, è un lavoro difficile ed oneroso, che richiede grande dispendio di tempo ed energia. Per tale motivo ai minatori viene riconosciuto un premio, ma solamente a coloro che sono stati in grado di minare un blocco. Tale premio è formato da due tipologie di incentivo:

- il primo incentivo consiste nell’ assegnazione di una certa quantità di moneta. Vengono assegnati 50 bitcoin per ogni blocco risolto, ma questo valore si dimezza ogni 210.000 blocchi;
- il secondo incentivo consiste nell’assegnazione delle commissioni incluse nel blocco stesso.

L’ offerta di moneta è limitata, infatti ogni 210.000 blocchi il numero di bitcoin viene dimezzato e, di conseguenza, tale offerta si esaurisce circa ogni 4 anni. Risulta facilmente comprensibile che questa prima tipologia di incentivo sia limitata per quantità sia per tempo. Per sostenere i costi dell’attività di mining è necessario che il prezzo dei bitcoin salga in modo significativo, oppure aumenti la seconda forma di incentivo. Le commissioni di transazione non sono obbligatorie e i minatori non hanno l’obbligo di processare tutte le transazioni, ma per avere la certezza che queste siano validate, è necessario

pagare questo incentivo. Tramite studi sui dati statistici, si è registrato un incremento percentuale del numero delle transazioni elevatissimo nel 2011, rilevando una crescita di oltre il 900%. Nel 2013 la crescita registrata è stata del 130%, minore rispetto all'anno precedente ma pur sempre elevata, tanto quanto negli anni successivi. Bitcoin è una tecnologia con enormi margini di miglioramento e con un vantaggio notevole, ovvero i costi di commissione molto più bassi rispetto a tutti gli strumenti di pagamento. Tramite i dati riguardanti le fee di transazione in bitcoin riguardo il periodo 2011-2014, si può notare che il totale delle commissioni pagate ammonta a circa 30.000 bitcoin, mentre i bitcoin scambiati ammontano a 29 milioni. Dividendo le commissioni per la quantità scambiata, otterremo un valore pari allo 0,10%, che oltre a rappresentare a quanto ammontano le commissioni che gravano sui bitcoin, esso rappresenta anche quanto siano inferiori rispetto alle richieste di altri mezzi di pagamento. Questi dati rendono quindi il bitcoin uno strumento privilegiato per tutte le transazioni finanziarie.

2.3 L'algoritmo di mining

Il mining è una sorta di competizione tra minatori per chi è il primo a trovare la risposta a un problema matematico che risolva il blocco. E'evidente, quindi, che la velocità nel ricercare una delle possibili soluzioni è l'aspetto peculiare dell'attività di mining, infatti quest'ultima è un'operazione di forza bruta in

cui si procede per tentativi applicando tutte le possibili combinazioni finché un minatore non vince. La differenza nella risoluzione del blocco è giocata dal Target. Il Target è un numero a 256 bit che può rappresentare differenti informazioni ed è espresso in scala esadecimale. Il suo valore si modifica in base alla differenza percentuale tra tempo effettivo e tempo teorico necessario per minare 2016 blocchi. Il protocollo Bitcoin prevede che il tempo teorico necessario per minare un blocco sia pari a 10 minuti, di conseguenza per minare 2016 blocchi sono necessarie circa 2 settimane. Tuttavia, la tempistica richiesta può essere più breve o più ampia rispetto a quella teorica. Nel caso in cui i minatori siano stati rapidi nel minare i blocchi, il Target si riduce e la successiva prova di lavoro risulterà più complicata, invece, nel caso opposto, ovvero quando i minatori impiegano più tempo per risolvere i blocchi, il Target incrementa e la prova successiva risulterà più facile. Da qui occorre parlare anche della Difficoltà, ovvero la misura di quanto sia complicato trovare un Hash al di sotto di un certo Target. Le principali caratteristiche sono:

- il valore iniziale è pari a 1;
- non ha un valore massimo;
- non può mai essere inferiore a 1;
- si aggiusta ogni 2016 blocchi, cioè ogni due settimane;
- è inversamente correlata al Target;

- è positivamente correlata all' Hash rate.

Ciò che risulta importante conoscere è il numero di giorni intercorsi tra i vari cambi di Difficoltà. In media il cambio di Difficoltà avviene ogni 12 giorni, con un minimo di tre ed un massimo di 17 giorni. I dati utilizzati per comprendere l'andamento progressivo dei cambi di Difficoltà risultano distribuiti in modo uniforme intorno alla media, offrendo grande stabilità. Partendo da questo è stato possibile arrivare ad una conclusione, ovvero la possibilità di stimare quando si verificherà quel determinato evento. Per terminare il discorso, è stato accennato anche l'Hash rate, ovvero la potenza complessiva, in Giga-Hash al secondo, che il network sta eseguendo. Si tratta di un valore enorme, in continua crescita esponenziale. Come già detto, esso ha una correlazione quasi perfetta con la Difficoltà. Se nel network aumenta la potenza di Hash è molto probabile che il tempo effettivo per la prova di lavoro diminuisca e sia inferiore rispetto a quello teorico, con la conseguenza che verrà aumentata la Difficoltà successiva. Tutto ciò giustifica come la potenza di Hashing sia in continua espansione e rispecchi gli investimenti effettuati.

CAPITOLO 3

GENERAZIONE DEI BITCOIN

In questo capitolo si procederà all'analisi che porterà a stimare il costo di produzione di un bitcoin. Per effettuare tale analisi verranno presi in

considerazione tre fattori: la spesa di capitale, la spesa operativa e il costo totale. Riguardo il primo fattore, se, teoricamente, si dividessero i 220 milioni GH/s in equivalenti BitMain AntMiner S3 ASIC (478 GH/s ciascuna), si otterrebbero circa 460,251 unità che al prezzo di $ 540 ciascuno risulterebbe una spesa totale pari a $ 248,5 milioni. Considerando il tasso di remunerazione di 25 bitcoin ogni 10 minuti, si ottiene una produzione di 1.314.900 bitcoin minati ogni anno. Da qui è possibile calcolare il CAPEX per bitcoin, ovvero quei fondi impiegati da un'impresa per acquistare asset durevoli:

CAPEX= $ 248,5 milioni/ 1,3149 milioni bitcoin = $189

Questo indicatore sarà utile per l'analisi, ma prima si passerà al secondo fattore, ovvero la spesa operativa. Con un Hash rate pari a 220 milioni GH/s la rete necessiterebbe di 1.476.235.200 KWh/anno. Nel caso in cui l'elettricità comporta costi pari a 70$/MWh si otterrà il nostro nuovo indice definito come OPEX con un valore pari a 103,33 milioni. Con OPEX si intendono i costi necessari per gestire un prodotto o un business e, facendo un calcolo simile a quello fatto con CAPEX, si otterrà il valore OPEX per bitcoin pari a:

OPEX= $ 103,33 milioni / 1,3149 milioni bitcoin = $ 79

Ora che i due indici sono stati evidenziati, si può passare al terzo fattore, il costo totale. Tramite la semplice somma dei CAPEX e OPEX si otterrà il costo mining per un bitcoin pari a:

CAPEX+OPEX = $ 189+ $79 = $ 268

I dati utilizzati dipendono da molti fattori e il calcolo del costo totale potrebbe discostarsi da quello effettuato, ma lo studio dei tre precedenti fattori potrà essere molto utile per comprendere, oltre il costo economico di produzione di bitcoin, gli impatti socio-ambientali legati alla loro produzione. Partendo dall' analisi economica, è di dominio comune il fatto che il costo legato alla produzione di moneta fisica in metallo per le valute a basso valore nominale sia superiore al valore della stessa. Il motivo di tale situazione è legata al costo sempre maggiore dei principali metalli utilizzati. Partendo da questi presupposti, è ovvio che l'impatto economico di una moneta fisica sia molto maggiore rispetto ad una criptovaluta, la quale non necessita di processi di lavorazione per essere ottenuta. Grazie a questo vantaggio, infatti, i costi di creazione di una moneta digitale sono pari, rispettivamente, all' 1% e al 3% nei confronti di oro e moneta. Una volta compreso il beneficio a livello economico della criptovaluta in generale, si può passare al confronto con gli impatti ambientali. Il confronto tra moneta digitale e fisica è enorme in questo ambito. Basti considerare gli enormi consumi di energia e le tonnellate di CO_2 introdotte nell'atmosfera, senza considerare i vari elementi legati alla produzione. L'unica fonte utilizzata nella produzione di bitcoin è l'energia elettrica, la quale, c'è da aggiungere, si sta spostando verso fonti sempre più rinnovabili. Per concludere, quindi, è molto facile comprendere i vantaggi di una moneta digitale rispetto alla moneta tradizionale e uno degli ostacoli che

certamente non sta permettendo a queste differenze di essere evidenziate è l'enorme disinformazione che il pubblico possiede in materia, ma mano a mano che la società si evolverà riuscirà maggiormente ad approcciarsi a determinati argomenti.

CAPITOLO 4

I MERCATI OTC

In questo capitolo verrà affrontato il funzionamento e le caratteristiche dei mercati all' interno dei quali i bitcoin vengono negoziati. I bitcoin sono scambiati su mercati non regolamentati, noti come mercati OTC (Over The Counter), i quali presentano le seguenti caratteristiche:

- sono mercati decentralizzati;
- sono privi di cassa compensazione;
- presentano ridotti costi di transazione;
- hanno un rischio maggiore rispetto ai mercati regolamentati.

Queste tipologie di mercati presentano una distinzione radicale rispetto a quelli tradizionali, infatti essi non possiedono una localizzazione fisica e le negoziazioni avvengono in maniera bilaterale su piattaforme o altri mezzi di comunicazione. Un mercato regolamentato, quindi, possiede una localizzazione precisa e, inoltre, presenta una disciplina relativa all' organizzazione, all'operatività e ai requisiti di quotazione. Tali regolamenti

sono approvati da un'autorità centrale, la quale svolge un ruolo di controllo, di vigilanza e di tutela del mercato. Le differenze esposte sono molteplici e ciò si traduce in un rischio maggiore per l'operatività su mercati OTC.

4.1 Il mercato Forex

Il Forex è un mercato OTC che presenta caratteristiche uniche rispetto agli altri mercati finanziari, in particolare si tratta di un mercato delocalizzato con possibilità di tradare 24 ore al giorno, esclusi i weekend. Inoltre, esso rappresenta il primo mercato mondiale per volumi di scambi e per numero di partecipanti attivi. Il cambio più tradato è il cross euro-dollaro, con una percentuale di mercato del 24%, seguitp dal cross dollaro-yen con un 18%. E' stato brevemente introdotto il mercato Forex per una ragione ben precisa, dato che presenta molti punti in comune con Bitcoin. Come già visto, i bitcoin non presentano gli elementi necessari per essere considerato una valuta, ma dal punto di vista del trading viene già negoziato come se lo fosse. Non a caso, viene quotato contro le principali valute su mercati OTC aperti 24 ore al giorno. Da quest'ultimo punto di vista, gli exchange del bitcoin rappresentano un'evoluzione dei tradizionali mercati finanziari, poiché è sempre possibile aprire una nuova posizione o liquidarne una già aperta in qualunque giorno dell'anno. Un mercato finanziario deve garantire tre gradi di efficienza:

- Tecnica: capacità di offrire bassi costi di transazione.

- Funzionale: capacità di far incrociare domanda e offerta.
- Informativa: capacità di riflettere sui prezzi tutte le informazioni disponibili.

Prendendo in considerazione i primi due punti, i bitcoin garantiscono un'efficienza elevata. Sono stati già discussi i vari vantaggi che possono essere offerti dai bitcoin ed è già nota quindi la bassa incidenza dei costi di transazione. Riguardo il terzo punto, l'efficienza informativa è altrettanto elevata e garantita da numerosi siti e account social che pubblicano in maniera tempestiva news e aggiornamenti. I principali cross tradati sui vari exchange sono:

- BTC/USD (dollaro americano);
- BTC/CNY (renminbi);
- BTC/EUR (euro);
- BTC/CAD (dollaro canadese);
- BTC/RUR (rublo russo);
- BTC/GBP (sterlina inglese);
- BTC/JPY (yen giapponese);

  Questa quotazione è di tipo "certo per incerto": si scambia un'unità di bitcoin (certa), assunta come base di cambio, per una quantità variabile di un'altra valuta (incerta). Il tasso di cambio è espresso come rapporto tra due valute in cui la valuta certa si trova al numeratore, mentre la valuta

incerta al denominatore. Ne deriva che un aumento della quotazione del tasso di cambio comporta che la stessa quantità di moneta certa possa acquistare una maggiore quantità di moneta incerta. In termini tecnici, si dice che la valuta certa si apprezza su quella incerta. In caso contrario, ovvero quando la quotazione del tasso di cambio diminuisce, la valuta certa si deprezza su quella incerta, portando la stessa quantità di moneta certa a poter acquistare una quantità minore di moneta incerta.

CAPITOLO 5

ANALISI DI PREZZO DEL BITCOIN

In questo capitolo si passerà all'analisi della serie storica dei prezzi bitcoin contro il dollaro americano. L' obiettivo sarà quello di fornire strumenti operativi che siano in grado di supportare le scelte di chiunque sia intenzionato ad avventurarsi nel settore. Il fattore chiave su cui basare la propria scelta è la propensione al rischio e il capitale da voler utilizzare. Sicuramente, nonostante ci si basa su dati e andamenti storici, non sarà mai possibile avere delle certezze riguardo gli investimenti, il rischio è alto, ma anche i profitti lo sono. Da qui, si procede ad analizzare il trend di lungo periodo. E' evidente che i prezzi sono in continua ascesa e ogni fase di rintracciamento è stata un'occasione di acquisto per il medio e lungo termine. Prendendo in considerazione il periodo che va dal 2010 al

2014, è stata registrata una crescita esponenziale: in soli quattro anni e mezzo il prezzo del bitcoin è passato da 0,0769 a $ 620, con una performance del 464.009%. L'unica prestazione negativa è avvenuta nel 2014, in cui la performance registrata ammonta a -52%. In questo lasso di tempo distinguiamo sei fasi:

- La prima fase è durata 298 giorni e si è conclusa con il massimo del 10 giugno 2011 a $ 35. La variazione percentuale è stata del 45.445%.
- La seconda fase è durata 164 giorni dal massimo della prima fino al minimo del 21 novembre 2011. I prezzi sono crollati, passando da $ 30 a $2,29, con una perdita del 92%.
- La terza fase è durata 505 giorni dal minimo della seconda al minimo del 9 aprile 2013. I prezzi hanno registrato un incremento del 10.027%, passando da $ 2,35 a $ 237,99.
- La quarta fase è durata 87 giorni dal massimo della terza al minimo del 5 luglio 2013. I prezzi sono diminuiti del 66% passando da $ 198 a $67,85.
- La quinta fase è durata 152 giorni dal minimo della quarta al massimo assoluto del 4 dicembre 2013 a $ 1151. I prezzi sono cresciuti del 1.560%.
- L'ultima fase è durata 178 giorni e va dal massimo della quinta al minimo del 10 aprile 2014, con una discesa dei prezzi del 27%.

Adesso verrà proposta un'analisi di tipo statistico riguardante il periodo in questione. Sui 1557 giorni analizzati, in 756 di essi il prezzo di chiusura è

stato superiore rispetto a quello della giornata precedente. Da questo emerge che le giornate positive e quelle negative sono praticamente bilanciate. C' è un aspetto interessante da tenere in considerazione, ovvero che nelle giornate positive i prezzi sono cresciuti ad un ritmo superiore rispetto alla decrescita nelle giornate negative. Ma questo non basta come base per un'analisi efficiente, infatti occorre tenere in considerazione la Difficoltà, la quale ha un forte legame con il prezzo. Tale legame è per la maggior parte del tempo positivo e, più alta sarà la Difficoltà, maggiore sarà il lavoro richiesto. Dal 17 agosto 2010 fino al 2014 sono avvenuti ben 127 cambi di Difficoltà accompagnati dalle relative variazioni dei prezzi che sono state riportate in precedenza. Spaccando le casistiche in variazioni percentuali negative e positive, si ha la conferma che le distribuzioni non sono né regolari né di facile interpretazione che porta il tutto ad essere non facilmente prevedibile. La domanda che ci si può porre è se sia sensato fare una sorta di previsione sui prezzi. La risposta è affermativa, ma è da tenere presente che, nonostante dati statistici alla mano, è pur sempre una previsione. L'andamento del prezzo del bitcoin dipende da domande ed offerta, come per qualsiasi altra attività, ma sappiamo anche che, nel caso dei bitcoin, anche la Difficoltà gioca il proprio ruolo nell'influire su tale andamento. Quando si è intenzionati a fare previsioni di lungo periodo, occorre anche distinguere la previsione del prezzo realizzata applicando la volatilità storica nei casi di variazione positiva della

Difficoltà rispetto alla previsione effettuata nei casi variazione negativa della Difficoltà. Il motivo è semplice, dato che la rilevanza statistica delle variazioni negative della Difficoltà è bassa. Come già detto, infatti, il legame tra prezzi e Difficoltà è per la maggior parte del tempo positivo. Nel periodo che abbiamo preso in considerazione, nel settembre del 2014 tale relazione è diventata negativa. In questo contesto, la Difficoltà continua ad aumentare mentre i prezzi restano in un trend ribassista. In ottica di lungo periodo è improbabile che questa correlazione non ritorni verso valori positivi e, affinché questo si verifichi, i prezzi dovranno necessariamente aumentare. A questo punto è chiaro che siano necessari strumenti e conoscenze adeguate per poter effettuare delle previsioni e infatti, nel prossimo capitolo, verranno introdotti i concetti base della cosiddetta "Analisi tecnica".

CAPITOLO 6

L' ANALISI TECNICA

L'analisi tecnica può essere definita come lo studio del movimento del mercato tramite l'uso sistematico dei grafici allo scopo di prevedere la tendenza futura dei prezzi. Due sono gli obiettivi da tenere in considerazione: obiettivi di tipo analitico e di tipo predittivo. L'obiettivo analitico viene

raggiunto attraverso lo studio che permette di comprendere il movimento dei mercati finanziari, mentre l'obiettivo predittivo si realizza attraverso la previsione rivolta a delineare i futuri andamenti. Nell'Analisi tecnica l'andamento dei prezzi può essere rappresentato utilizzando varie tipologie di grafici:

- Grafico lineare.
- Grafico a barre.
- Grafico a candele.

Per quanto riguarda i primi due, la costruzione dei grafici è piuttosto comune, dato che prevedono l'esistenza di un piano cartesiano con i due assi che rappresentano il tempo in ascissa e il prezzo in ordinata. Il terzo grafico è differente rispetto agli altri due e può anche essere definito migliore, sia per completezza, sia per facilità di visualizzazione, quindi verrà focalizzata l'attenzione maggiormente su quest'ultimo.

6.1 Il grafico a candela

I dati essenziali per un grafico a candela sono quattro:

- Apertura (Open)
- Massimo (High)
- Minimo (Low)
- Chiusura (Close)

Tramite questi quattro elementi è possibile costruire la candela, la quale si compone di un corpo (Real Body), un'ombra superiore (Upper Shadow) e un'ombra inferiore (Lower Shadow). Il corpo è dato dalla differenza tra pezzo di chiusura e pezzo di apertura. Se la differenza tra le due è positiva, allora la candela rappresenta un movimento rialzista dei prezzi e per convenzione il body è di colore bianco. Al corpo si aggiunge l'ombra superiore, data dalla differenza tra prezzo massimo e prezzo di chiusura, e l'ombra inferiore, data dalla differenza tra prezzo di apertura e prezzo minimo. Se la differenza tra prezzo di chiusura e prezzo di apertura è negativa, allora la candela rappresenta un movimento ribassista dei prezzi e per convenzione il body è di colore nero. Anche in questo caso al corpo si aggiunge l'ombra superiore, data però dalla differenza tra prezzo massimo e prezzo di apertura, e l'ombra inferiore, data dalla differenza tra prezzo di chiusura e prezzo minimo.

6.2 I principi fondamentali dell'analisi tecnica

I presupposti su cui si fonda tutta l'Analisi tecnica sono tre:

- il mercato sconta tutto;
- i prezzi si muovono in un trend;
- la storia si ripete.

Riguardo il primo presupposto, non c'è molto da dire rispetto a quello che è già noto. Nei prezzi sono già incorporati tutti quei fattori di tipo fondamentale, politico, economico e monetario che ne hanno determinato il prezzo. Il prezzo si modifica in base alla domanda dei compratori e all'offerta dei venditori. Questi sono concetti base: i prezzi sono in equilibrio quando l'offerta è supportata dalla domanda, aumentano quando la domanda è superiore all' offerta e diminuiscono quando l'offerta è maggiore della domanda. Riguardo il secondo presupposto, l'Analisi tecnica ha lo scopo di identificare un trend fin dai primi momenti, cercando di investire nella sua direzione fino al suo esaurimento. Il trend è l'orientamento di una certa serie di valori a crescere, diminuire o non subire significative variazioni nell'arco di un determinato periodo di tempo. Si può sintetizzare come l'indicazione della direzione dei prezzi. Infine abbiamo il terzo presupposto, una conseguenza dello studio dell'andamento dei prezzi da parte dell'Analisi tecnica. Non è infatti impossibile che la "storia si ripeta" in determinati momenti di mercato, generando i cosiddetti pattern. I pattern sono dei veri e propri modelli che si ripetono nel tempo. Se individuati correttamente, possono fornire maggiori probabilità e indicazioni per comprendere l'evoluzione futura delle quotazioni. Dopo essere entrati nell'ottica dell'Analisi tecnica, aver elencato le modalità di rappresentazione tramite grafici e i presupposti su cui si fonda, è arrivato il momento di introdurre i due concetti fondamentali: supporti e resistenze.

6.3 Supporti e resistenze

Supporti e resistenze sono i concetti cardine per l'Analisi tecnica. Il supporto è un particolare livello di prezzo attorno al quale le correnti di domanda hanno la capacità di arrestare la flessione dei prezzi. Un livello di supporto sul quale si arresta la discesa dei prezzi fornisce un potenziale segnale di acquisto, in quanto indica una maggiore presenza di compratori rispetto ai venditori. La decisa rottura al ribasso di un livello di supporto, invece, rappresenta un segnale di vendita, indicando una presunta incapacità dei compratori nel fronteggiare la forza predominante dei venditori. La resistenza è un particolare livello di prezzo attorno al quale le correnti di offerta hanno la capacità di arrestare l'ascesa dei prezzi. Un livello di resistenza sul quale si arresta la salita dei prezzi fornisce un potenziale segnale di vendita, in quanto indica una maggiore presenza di venditori rispetto ai compratori. Tuttavia, la decisa rottura al rialzo di un livello di resistenza rappresenta un segnale di acquisto, indicando una presunta incapacità dei venditori nel fronteggiare la forza predominante dei compratori. I livelli di supporto e resistenze possono essere di tipo statico, cioè, una volta fissati, il prezzo non varia in base al passare del tempo. Questi livelli però possono essere anche di tipo dinamico, e in tal caso si parla di trendline. Un trendline è una linea retta che passa per almeno due punti di massimo e di minimo con lo scopo di rendere evidente il trend del

mercato. Il trendline rialzista è tracciato congiungendo almeno due minimi, di cui il secondo è più alto, e funge da supporto dinamico ai prezzi. Il trendline ribassista è tracciato congiungendo almeno due massimi, di cui il secondo è più basso, e funge da resistenza dinamica ai prezzi. Sia per i livelli statici sia per quelli dinamici valgono le seguenti considerazioni:

- l'affidabilità risulta maggiore quanto più elevato è il numero di contatti tra i prezzi e la linea;
- l'inversione di tendenza si verifica quando viene identificato il definitivo breakout della linea e prende avvio una nuova fase di mercato.

6.4 Le medie mobili

Lo strumento più utilizzato da parte dell'Analisi tecnica è dato dalle medie mobili. Esse sono utili sia per regolare la serie temporale, processo conosciuto come smoothing, sia per individuare segnali operativi di gestione di posizioni speculative. Introduciamo tre tipologie di medie mobili:

- medie mobili semplici – SMA;
- medie mobili ponderate – WMA;
- medie mobili esponenziali – EMA;

La media mobile semplice è la più utilizzata e si costruisce tramite una media aritmetica di N osservazioni, aggiornata nel tempo con l'eliminazione dal dato più remoto e l'aggiunta di quello più recente. In generale una media mobile di

dominio N elimina le componenti erratiche di periodo minore o uguale a N, pertanto medie mobili semplici calcolate su ampi domini operano un più accentuato livellamento della serie perequata. Per questo motivo le medie mobili di periodi lunghi fungono da supporti/resistenze molto attendibili. Può risultare opportuno pesare in modo diverso i prezzi, come viene fatta nella media mobile ponderata. La ponderazione riduce il ritardo rispetto alla media mobile semplice. Per l'attribuzione dei pesi si segue generalmente il metodo lineare, moltiplicando l'ultimo termine per N. Una ponderazione più raffinata, che evita la perdita di dati caratterizzante le due precedenti elaborazioni di medie mobili, si ottiene attraverso la perequazione esponenziale. Quest'ultima consente di conservare l'effetto anche dei dati più remoti che non è mai stato annullato del tutto. Adesso che sono state introdotte le medie mobili, si può passare ad introdurre nuovi indicatori essenziali per l'Analisi tecnica.

6.5 Le bande di Bollinger

Per costruire le Bande di Bollinger si parte con la misurazione di una tendenza centrale e, successivamente, con una banda superiore e una banda inferiore. La misura della tendenza centrale deve essere una media mobile semplice e l'intervallo deve essere delineato attraverso una misura di volatilità, utilizzando la deviazione standard, statisticamente definita come scarto quadratico medio o radice quadratica della varianza. Entrambe le due

misurazioni (media mobile e deviazione standard) vengono calcolate sullo stesso intervallo temporale, che di dafault Bollinger stesso fissa a 20 giorni. A tale media mobile viene aggiunto e sottratto due volte il valore della deviazione standard. Così facendo si creano due bande, una superiore e una inferiore, che, per costruzione, contengono sempre al loro interno una media mobile. Il punto di forza di queste Bande è la loro capacità di essere in grado di adattarsi a ogni contesto di mercato e mantenere sempre una valida definizione di ciò che è "alto" e di ciò che è "basso". Le Bande di Bollinger danno segnali di acquisto e vendita quando si verificano le seguenti condizioni:

- Se il prezzo esce dalla banda superiore e successivamente vi rientra, si ottiene un segnale di vendita. Questo corrisponde a un rapido aumento del prezzo e a un successivo rallentamento o aggiustamento.
- Se il grafico del prezzo esce dalla banda inferiore e successivamente vi rientra, si ottiene un segnale di acquisto, cioè il prezzo è calato molto velocemente fino ad arrestarsi e potrebbe essere pronto a investire il trend.

Per concludere la trattazione sulle Bande di Bollinger occorre precisare che sarebbe errato utilizzare semplicisticamente i segnali di acquisto o vendita quando si raggiunge un limite estremo e in quel momento settare il prezzo obiettivo sulla media. Per questi motivi è consigliato utilizzare altri indicatori

con le Bande, con lo scopo di aumentarne l'efficacia ed eliminare i falsi segnali. Tali indicatori sono noti come "%b" e "BandWidth".

6.6 Il Percentage B o "%b"

Il "%b" è un indicatore costruito a partire dalle Bande di Bollinger ed è in grado di determinare dove si trova il prezzo in relazione alle Bande stesse. Il suo valore è pari a:

- 1 quando il prezzo tocca la banda superiore;
- 0,5 quando il prezzo si trova sulla media;
- 0 quando il prezzo tocca la banda inferiore.

6.7 Bandwidth

Questo indicatore è fondamentale per poter individuare le situazioni in cui la volatilità ha raggiunto un livello così basso da farne prevedere un'inversione imminente del trend. Il suo utilizzo più semplice è quello di verificare quando tocca il minimo degli ultimi sei mesi, poiché è estremamente probabile che la volatilità dei prezzi possa aumentare. Non a caso, quasi tutti i più importanti trend nascono quando il BandWidth ha valori piuttosto bassi. La sua ultima e più importante capacità è quella di identificare la fine di un trend. Se l'inizio è, infatti, sostenuto da un aumento del BandWidth, una sua flessione dà un primo campanello di allarme che il trend è prossimo all'esaurimento.

6.8 Il Williams %R

Si introdurrà un altro indicatore, il penultimo della nostra analisi, ma non di minore importanza. Tale indicatore rientra nella categoria degli oscillatori. Con questa affermazione ci si riferisce a elementari elaborazioni quantitative della serie dei prezzi volte a isolare determinate caratteristiche di velocità, forza o volatilità delle quotazioni rispetto al rapporto tra forze bullish (in acquisto) e bearish (in vendita). Il Williams %R riflette il livello della chiusura rispetto al massimo tra i massimi toccati dal prezzo e va a confrontare tale misura rispetto al più ampio range degli ultimi N periodi. Tale valore viene moltiplicato per -100, al fine di dare all'oscillatore una lettura visiva concorde al movimento del prezzo. L'indicatore oscilla tra 0 e -100. Se il suo valore è compreso tra -80% e -100% significa che ci si trova in una situazione di ipervenduto, nelle quali il prezzo di chiusura è molto vicino al minimo e le forze in vendita prevalgono rispetto a quelle di acquisto. Un valore compreso tra 0% e -20% indica una situazione di ipercomprato, nelle quali il prezzo di chiusura è molto vicino al massimo e segnala che i compratori prevalgono rispetto ai venditori. Per ottenere informazioni pulite da questo indicatore è necessario associarlo all' interno di un trading system insieme ad altri indicatori che possano fungere da filtro per aiutare a distinguere se ci si trova in presenza di una fase di inversione o di continuazione del trend.

6.9 Il Parabolic SAR

Il SAR è l'ultimo indicatore che verrà trattato. La caratteristica unica di questo strumento è l'assenza di base temporale, cioè la sua costruzione non si basa su parametri di tempo ma su variazioni di volatilità dei prezzi. Inoltre il SAR prevede come input solo un fattore di accelerazione compreso tra 0,02 e 0,20. La formula è di tipo iterativo e si costruisce sommando il SAR precedente la differenza, moltiplicata per il fattore di accelerazione, tra il punto estremo e il SAR precedente. Da un punto di vista grafico, il SAR si presenta come una serie di punti posizionati al di sopra o al di sotto dei prezzi. Da questo è facile comprendere che se i punti del SAR si trovano al di sopra dei prezzi, segnalano un trend ribassista (down trend) e in questa situazione l'indicatore funge da resistenza dinamica dei prezzi. Invece, quando i punti del SAR si trovano al di sotto dei prezzi, essi segnalano un trend di tipo rialzista e in questa situazione l'indicatore funge da supporto dinamico ai prezzi. Per concludere il capitolo, si definisce il SAR come un true reversal system, cioè un sistema di trading tale per cui ogni punto di stop è anche un punto di inversione.

CAPITOLO 7

TRADING SYSTEM E BITCOIN

Il Trading System è un sistema automatico di elaborazione delle informazioni riguardanti un insieme di strumenti finanziari che fornisce dei segnali operativi, cioè le indicazioni sugli ordini di acquisto e vendita da immettere nel mercato. In questo capitolo si parlerà dei sistemi di trading automatici applicando gli strumenti di Analisi tecnica esposti nel precedente capitolo. E' da precisare che si tratta di un campo in cui sono richieste competenze avanzate di Analisi tecnica, ma soprattutto di statistica e programmazione. Le regole generali per tutti i trading system sono le seguenti:

- Se il segnale viene generato il giorno T si entra in posizione a mercato al prezzo di apertura del giorno T+1.
- La quantità di bitcoin che verrà comprata o venduta a mercato è calcolata dividendo il capitale disponibile al giorno T per il prezzo di chiusura.
- Assumendo i costi di slippage (ovvero il costo nascosto dovuto alla differenza che si registra tra il prezzo di mercato e il prezzo effettivo di esecuzione) pari all' 1% per rispecchiare l'elevata volatilità del mercato.
- Costi di commissione pari a zero.
- L'intervallo temporale in considerazione sarà dal 21/05/2012 fino al 21/11/2014.

7.1 Trading system con le medie mobili

Per costruire un trading system tramite medie mobili utilizzeremo i seguenti parametri:

- media mobile semplice a 5 giorni;
- media mobile semplice a 10 giorni;
- ingresso long quando la media mobile semplice a cinque giorni taglia il basso verso l'alto la media mobile semplice a dieci giorni;
- ingrasso short quando la media mobile semplice a cinque giorni taglia dall' alto verso il basso la media mobile semplice a dieci giorni.

Costruendo il trading system, si noterà che durante i primi giorni dell'agosto 2013, a seguito del taglio dal basso verso l'alto della media mobile semplice a cinque giorni, il trading system ha lanciato un segnale di acquisto (posizione long). La posizione viene mantenuta con profitto per circa due settimane quando un nuovo taglio, questa volta dall'alto verso il basso, fa chiudere in profitto la posizione long e contemporaneamente viene lanciato dal trading system un segnale di vendita (posizione short). Questa nuova posizione viene chiusa in leggera perdita dopo poche sedute, quando il segnale rialzista apre un nuovo segnale long. Ipotizzando di partire da un capitale iniziale di $ 10.000, si nota che il trading system di quel periodo ha generato 60 segnali, di cui venti sono stati chiusi a profitto e 40 in perdita. Ne deriva che la

percentuale di profittabilità è del 33%, tuttavia il profitto ottenuto è di $ 216.307, perché l'utile medio ($21.877) supera la perdita media ($ -5.531).

7.2 Trading system con le Bande di Bollinger

I parametri che verranno utilizzati sono:

- 20 giorni come periodo di osservazione;
- ingresso long quando il prezzo rompe la Banda superiore di Bollinger;
- ingresso short quando il prezzo rompe la Banda inferiore di Bollinger.

Il 3 marzo 2014 il prezzo ha rotto con decisione la Banda superiore e il trading system genera un segnale di acquisto sotto la rottura al prezzo di $ 685. Non si dimostra un'operazione vincente e il 21 marzo la posizione viene chiusa alla rottura al prezzo di $ 569. Sulla base delle regole fissate, la posizione long non viene chiusa ma viene aperta immediatamente una posizione short.

Ipotizzando nuovamente un capitale iniziale di 10.000, si nota che, costruendo il trading system, esso genererà 20 segnali, di cui 11 chiusi a profitto e 9 in perdita. In questo caso la percentuale di profittabilità è più alta, pari al 55%, generando un profitto totale di $ 576.558.

7.3 Trading system con il Williams %R

I parametri selezionati sono:

- periodo di osservazione: 14 giorni;
- ingresso long quando il Williams rompe dal basso verso l'alto il livello di ipercomprato;
- ingresso short se il Williams rompe dall'alto verso il basso il livello di ipervenduto.

Il 28 aprile il Williams è sceso sotto il livello -80%, generando un segnale di vendita pari a $430. Tale operazione è stata chiusa in perdita il 21 maggio a $ 489 e, contestualmente, viene aperta una posizione long allo stesso livello di prezzo. Questa posizione viene mantenuta fino al 13 giugno, quando in seguito alla rottura del livello viene generato il segnale di uscita con un significativo profitto. Restando a mercato, si apre immediatamente una posizione short che viene chiusa il 1° luglio a $ 642. La posizione long successiva che si genera viene chiusa il 26 luglio 2014 a $ 600, data in cui si entra short, e alla data finale è ancora in posizione short con il bitcoin che ha raggiunto i $ 350. Tornando all'ipotesi di avere a disposizione un capitale iniziale pari a $ 10.000, il trading system in questo caso ha generato 23 segnali nel periodo in considerazione, di cui 12 sono stati chiusi in profitto e 11 in perdita. La percentuale di profittabilità ammonta al 52% e il profitto totale è pari a $ 760.827.

7.4 Trading system con il Parabolic SAR

In quest'ultimo caso verranno imposte le seguenti regole:

- ingresso long quando il livello di prezzo rompe al rialzo l'indicatore SAR;
- ingresso short quando il livello di prezzo rompe al rialzo l'indicatore SAR.

Ad inizio ottobre 2014 il prezzo del bitcoin interrompe il trend ribassista che ha caratterizzato il mese di settembre e il trading system genera un segnale di acquisto. La posizione viene mantenuta per un paio di settimane e chiusa in profitto. Nello stesso istante la rottura al ribasso del SAR genera un segnale di vendita e anche questo trend viene catturato con successo fino a quando l'ulteriore rottura del SAR al rialzo fa ribaltare nuovamente la posizione. Considerando sempre l'ipotesi del capitale iniziale di $ 10.000, il trading system in questo caso ha generato 54 segnali, di cui 31 chiusi a profitto e 23 in perdita. Ne deriva una percentuale di profittabilità del 50% e un profitto totale pari a $ 190.685.

CONCLUSIONI

Con il capitolo “Trading system e Bitcoin” chiudiamo l’analisi sui bitcoin. L’obiettivo iniziale è stato raggiunto, i principi base di questa criptovaluta sono stati inquadrati, così come le funzionalità dei server, i ruoli dei vari utenti all’interno del network e l’applicazione all’interno dei mercati. Inoltre, sono stati elencati i più importanti indici che permettono di prevedere gli andamenti del prezzo, in modo tale che chiunque possa addentrarsi nelle mente di un vero trader e poter comprendere il ragionamento da compiere prima di investire. Comunque, come già citato durante i capitoli, occorrono delle conoscenze profonde in materia per poter applicare i modelli presentati, infatti il rischio di operare in questi mercati è commisurato alla preparazione personale, maggiori sono le nozioni a disposizione, maggiori sono le possibilità di poter avere un vero e proprio profitto tramite Bitcoin. Il mondo sta entrando in un’era in cui non bisogna sottovalutare le potenzialità di strumenti come Bitcoin, chi non si aggiorna rischia di rimanere indietro, l’era del digitale non fa sconti a nessuno e questo deve essere un chiaro messaggio per chiunque riesca a comprendere tale situazione. Nella parte iniziale sono stati indicati i numerosi vantaggi che questa valuta offre, ma c’è da dire che questi ultimi sono una conseguenza del fatto che la valuta sia legata ad una forma digitale. E’ proprio questo un altro aspetto che la tesi vuole mettere in risalto, ovvero la capacità di cambiamento che possono portare le tecnologie. L’evoluzione è alla base di tutto, in origine

l’unica modalità di scambio che l’uomo aveva a disposizione era il baratto, successivamente fu introdotta la moneta e dopo interminabili fasi storiche siamo arrivati alle valute che tutt’ oggi conosciamo. Il ragionamento di base è facile da comprendere, anche la moneta ha un suo processo di evoluzione ed è per questo motivo che diventa necessario prestare maggiore attenzione a strumenti come i bitcoin perché un giorno potrebbero essere talmente diffusi da sostituire la moneta corrente.

BIBLIOGRAFIA

- Criptovalute: manuale di sopravvivenza, Emanuele Florindi
- Bitcoin Facile, Cristian Palusci
- Bitcoin: Dalla teoria alla pratica, Alessio Barnini, Alessandro Aglietti
- Capire Blockchain, Lorenzo Foli
- Investire Bitcoin, Stefano Pepe

SITOGRAFIA

- www.tradingsystems.it
- www.fxempire.it
- www.blockchain4innovation.it
- www.ilsole24ore.com
- www.wired.it

RINGRAZIAMENTI

Ora che il percorso è concluso, vorrei citare le persone a me care a cui vorrei dedicare il titolo conseguito. Innanzitutto ringrazio la mia famiglia, i primi ad incitarmi nella scelta del percorso universitario e ad aver creduto di essere all'altezza per poter arrivare alla fine. Ringrazio i miei amici, il Bunker, con cui ho passato i miei migliori momenti e sono sempre stati in attesa che raggiungessi questo risultato. Più di tutti, ovviamente, un ringraziamento a me stesso per aver terminato questi anni di studio senza gli "aiutini" che molti altri hanno ricevuto. Per concludere, un ringraziamento speciale ad HAKEEEMEEE, la mia fonte di ispirazione passata e futura.